Chapter 20
A Collaborative Cybersecurity Education Program

Teemu J. Tokola
University of Oulu, Finland

Thomas Schaberreiter
University of Vienna, Austria

Gerald Quirchmayr
University of Vienna, Austria

Ludwig Englbrecht
https://orcid.org/0000-0002-8546-3017
University of Regensburg, Germany

Günther Pernul
University of Regensburg, Germany

Sokratis K. Katsikas
https://orcid.org/0000-0003-2966-9683
Norwegian University of Science and Technology, Norway & Open University of Cyprus, Cyprus

Bart Preneel
Katholieke Universiteit Leuven, Belgium & imec, Belgium

Qiang Tang
Luxembourg Institute of Science and Technology, Luxembourg

ABSTRACT

This chapter presents an implementation of a cybersecurity education program. The program aims to address some issues identified in current cybersecurity teaching in higher education on a European level, like the fragmentation of cybersecurity expertise or resource shortage, resulting in few higher education institutions to offer full degree programs. As a result of the Erasmus+ strategic partnership project SecTech, the program tries to overcome those issues by introducing collaborative development to cybersecurity education. SecTech lays the foundations for a collaborative education program, like the definition of a clear content, module and delivery structure, and the appropriate tool support to facilitate collaboration and content reuse. Additional effort is required to achieve long-term success, including the creation of a community that drives the content creation and maintenance, as well as an independent governance structure to steer the project in the long-term. While the project focuses on European collaboration, a global community is envisioned.

THE NEED FOR COLLABORATIVE CYBERSECURITY EDUCATION

Given the mounting cyber threat levels Europe is faced with, a coordinated cybersecurity education effort becomes more urgent than ever. The malware waves hitting Europe in May 2017 and recent Europol reports (European Union Agency for Law Enforcement Cooperation (Europol), 2017) give a clear warning of the dangers lying ahead, ranging from criminal activities to often state sponsored theft of intellectual property and a rising possibility of cyber sabotage. It is against this background that building on the EU cybersecurity strategy (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013), new legislation aimed at strengthening privacy protection (THE COUNCIL OF THE EUROPEAN UNION, 2016) – the General Data Protection Regulation (GDPR) - and securing IT-dependent critical infrastructures (THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016) – the directive on security of network and information systems (NIS) - was introduced. Both GDPR and NIS have come into effect in 2018. The obligations introduced by this legislation at European level have also increased the demand for cybersecurity experts in an already overstretched market. It is obvious that an increased supply of talent becomes an absolute necessity if Europe as a whole aspires to meet the high aims set in the legislation and in European and national cybersecurity strategies. However, a joint and well-coordinated European approach to education in this field is still missing. Given the variety and diversity of topics that need to be covered, comprising such diverse areas as information and communications technology, management and organization, law, economics, sociology, criminology and psychological issues, it becomes painstakingly clear that a wide range of expertise needs to be accessed to create a thorough curriculum. That is one major reason for comprehensive academic programs on cybersecurity and privacy being a rare exception.

In line with those developments the Erasmus+ strategic partnership project SecTech was formed by seven European higher education institutions (KU Leuven, Luxembourg Institute of Science and Technology, Norwegian University of Science and Technology, University of Oulu, University of Plymouth, University of Regensburg, and University of Vienna) to collaboratively develop a European cybersecurity curriculum. The core motivation of the Erasmus+ SecTech project is to provide a seed curriculum including ready to use on-line teaching materials to give European academic institutions a much better starting point for implementing and delivering a cybersecurity education program, either on their own or in cooperation with other institutions. The primary contributions this project is aimed at supporting are the integration of knowledge that is currently available across Europe, but today is hardly combined and far from being integrated, the introduction of a curriculum template, the provision of seed on-line course material that can serve as a core and finally the establishment of an on-line repository and cooperation platform that can serve as basis for a Europe wide joint educational effort. As the free sharing of the developed course materials is expected to have an essential impact, established open standards and systems such as Moodle and SCORM will form the technological basis.

With information and cybersecurity experts becoming an increasingly scarce resource, the pooling and sharing of teaching materials at a European level is expected to have a significant impact on enabling in a first step the participating universities and in a following expansion phase other tertiary level institutions to much easier offer credible cybersecurity degree programs and to incorporate modules or parts of modules in existing computer science and information systems programs. While in the course of the project we have not given specific focus on determining the advantages of such a curriculum for learners, one of the most obvious advantages is a more complete learning experience due to more

Related Content

Now What?: A Case Study on the Impact of Nefarious Queen Bees
Caroline M. Crawford (2023). *Addressing the Queen Bee Syndrome in Academia (pp. 1-25).*
www.irma-international.org/chapter/now-what/327164

Hardware-Free Network Internals Exploration: A Simulation-Based Approach for Online
Computer Networking Course
Qian Liu (2024). *International Journal of Innovative Teaching and Learning in Higher Education (pp. 1-16).*
www.irma-international.org/article/hardware-free-network-internals-exploration/339002

Not Another Discussion Board: One Online Instructor's Reflective Practices to Create Effective
Student Engagement
Elodie J. Jones (2024). *Balance and Boundaries in Creating Meaningful Relationships in Online Higher
Education (pp. 314-327).*
www.irma-international.org/chapter/not-another-discussion-board/335548

The Effect of Psychological Safety on the Performance of Students in Graduate-Level Online
Courses
George Hanshawand Jacob Hanshaw (2023). *International Journal of Innovative Teaching and Learning in
Higher Education (pp. 1-21).*
www.irma-international.org/article/the-effect-of-psychological-safety-on-the-performance-of-students-in-graduate-level-
online-courses/333864

"The Fact That the Author Was Male Instead of Female Provided for an Objective Opinion":
Implicit Bias in the Classroom
Julia Ferrara Waity, Jennifer Vandermindenand Kristin Robeson (2020). *International Journal of Innovative
Teaching and Learning in Higher Education (pp. 44-60).*
www.irma-international.org/article/the-fact-that-the-author-was-male-instead-of-female-provided-for-an-objective-
opinion/265506